

IN THE UNITED STATES DISTRICT COURT
FOR NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF
INFORMATION THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE,
1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA 94043

FILED UNDER SEAL

Case No. 20-mj -5-AJ

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Wesley R. Garland being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since May 2019. I am currently assigned to the Joint Terrorism Task Force (“JTTF”) of the FBI’s Boston Division/ Bedford,

New Hampshire office. Before I became a Special Agent, I was a Police Officer in Virginia for nine years. Over my career, I have investigated and assisted investigations of robberies, burglaries, larcenies, assaults, and murders. During my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants.

3. The facts in this affidavit come from my personal knowledge, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 2113, bank robbery, was committed by an unknown person. There is also probable cause to search the information described in Attachment A for evidence of this crime further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTES

6. *Hobbs Act Robbery*. Title 18, United States Code section 1951 states in relevant part,

Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any

person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.

7. The term “robbery” means:

[T]he unlawful taking or obtaining of personal property from the person or in the presence of another, against his will, by means of actual or threatened force, or violence, or fear of injury, immediate or future, to his person or property, or property in his custody or possession, or the person or property of a relative or member of his family or of anyone in his company at the time of the taking or obtaining.

18 U.S.C. § 1951(b)(1).

8. *Bank Robbery.* Title 18, United States Code section 2113 states in relevant part,

Whoever, by force and violence, or by intimidation, takes, or attempts to take, from the person or presence of another, or obtains or attempts to obtain by extortion any property or money or any other thing of value belonging to, or in the care, custody, control, management, or possession of, any bank, credit union, or any savings and loan association . . . [s]hall be fined under this title or imprisoned not more than twenty years, or both.

18 U.S.C. § 2113(a).

9. In addition, “[w]hoever, in committing, or in attempting to commit” the offense described above “assaults any person, or puts in jeopardy the life of any person by the use of a dangerous weapon or device, shall be fined under this title or imprisoned not more than twenty-five years, or both.” 18 U.S.C. § 2113(d).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

10. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other infrastructure.

Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers, and as a result information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

11. Based on my training and experience, I also know that most cellular devices have the capability to connect to wireless Internet (“wi-fi”) access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device’s wi-fi settings.

12. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that are within range.

13. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system (“GPS”) technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app’s operation.

14. Based on my training and experience, I know that Google is a company that, among other things, offers numerous online-based services, including email (Gmail), navigation

(Google Maps), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and Youtube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.

15. In addition, based on my training and experience, I know Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

16. Based on my training and experience, I know that, in the context of mobile devices, Google’s cloud-based services can be accessed either via the device’s Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

17. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user’s location, to determine the user’s location when Google Maps is used, and to provide location-based advertising.

18. In addition to the information that Google collects directly from users of their services, Google passively collects location data and other identification data from users. For instance, in the regular course of business, Google collects data from smartphone users that use its mobile applications (e.g., Gmail, Google Maps, the Google App), users that use Android devices, and even users that use other applications that incorporate the digital advertising tools that Google provides to advertisers and publishers. Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app.

19. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device. Google blends those sources of data together to create user profiles. Google provides some information about users for free, through their Google Analytics tools. But much of this data is collected and sold for profit or used (i.e. to deliver targeted advertising opportunities to companies' advertising through Google using their AdSense network). In the third quarter of 2018, Google's revenue from advertising reportedly accounted for \$24.1 billion of its overall \$27.77 billion revenue. Thus, Google has a business incentive to, and does, gather location and user data in a variety of ways through a number of techniques. And while location information for users of Android devices is particularly robust, through the prolific nature of its services and analytical tools for advisers and publishers, Google is able to gather this data for a substantial number of smartphone users.

20. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculcate or exculpate a Google account holder by showing that he was (or was not) near a given location at a time relevant to the criminal investigation.

21. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

22. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other

log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

23. As described below, there is probable cause that the same unidentified male subject committed three armed robberies between Monday, December 2, 2019, and Saturday, December 21, 2019.

A. Monday, December 2, 2019 (Rapid Refill Robbery).

24. At approximately 8:53 p.m. on Monday, December 2, 2019, an unidentified male subject (UNSUB) entered Rapid Refill, New Hampshire.

25. According to Google Maps, Rapid Refill, New Hampshire, is located approximately at the following latitude and longitude:

26. Rapid Refill sells goods that travel in interstate commerce.

27. Victim store clerk advised the Manchester Police that UNSUB walked into the store with a dark grey revolver in his waistband. The victim store clerk described UNSUB as a black male, approximately 5’ 8” to 5’ 9”, wearing a green hoody, light colored hat, jeans, and black gloves, with a scarf covering his face and a dark grey revolver in his waistband.

28. UNSUB pointed the firearm at the victim store clerk and asked him for money in the register and the store safe. The victim store clerk told UNSUB the safe has a 10 minute delay once the code is entered. UNSUB advised the victim store clerk he would wait.

29. At one point, another customer entered the store and approached the counter with items he was going to purchase. UNSUB told the customer he would take care of his purchase and he was good to leave.

30. Victim store clerk advised UNSUB left with approximately \$3,000.00-\$4,000.00 from the safe and approximately \$200.00 in mixed bills from the register.

31. The Manchester Police Department responded and, among other things, obtained video of the robbery.

B. Saturday, December 21, 2019 (Shell Gas Station Robbery).

32. At approximately 12:25 a.m. on Saturday, December 21, 2019, victim store clerk was standing outside the Shell Gas Station, New Hampshire when she observed a male jogging towards her from the West with a black, double barreled shotgun in his hand.

33. According to Google Maps, Shell Gas Station, New Hampshire, is located approximately at the following latitude and longitude:

34. The Shell Gas Station sells goods that travel in interstate commerce.

35. Victim store clerk described UNSUB as 5'6", scrawny, grey hooded sweatshirt with the hood up, black pants, black bandanna covering his face, and what appeared to be white foundation make up on the upper portion of his face.

36. Victim store clerk said UNSUB told her to come open the registers and safe. Victim store clerk walked towards the registers and advised UNSUB she did not have access to the safe. Victim store clerk retrieved approximately \$186.00 in unknown denominations from the register and gave it to UNSUB. Victim store clerk observed UNSUB take approximately

\$120.00 in unknown denominations from her purse. UNSUB asked victim store clerk to open the second register and lottery. Victim store clerk advised UNSUB she did not have access to the lottery. Victim store clerk gave UNSUB approximately \$100.00 in unknown denominations from the second register.

37. Victim store clerk advised that a victim patron entered the store and UNSUB ordered victim patron to the ground. UNSUB ordered victim patron to give him everything he had on him. UNSUB took everything victim patron removed from his pockets and left the gas station.

38. The Manchester Police Department responded and, among other things, obtained video of the robbery.

C. Saturday, December 21, 2019 (Bank of New England Robbery).

39. At approximately 8.00 a.m. on Saturday, December 21, 2019, UNSUB entered the Bank of New England, New Hampshire.

40. According to Google Maps, the Bank of New England, New Hampshire, is located approximately at the following latitude and longitude:

41. UNSUB was seen on camera driving around the bank at around 7:40 a.m. in a white hatchback. He stopped at the drive-thru ATM with no garments covering his face. He parked the vehicle in the parking lot on the side of the bank. UNSUB entered the side door of the bank after the victim manager unlocked the door. UNSUB approached the victim manager and victim teller and had what appeared to be a double barrel shotgun in his hand that he waved around.

42. UNSUB was described by the victim manager as a black male wearing white face makeup and what looked to be a black wig. He wore a dark knit beanie, blue scarf over the lower part of his face, grey sweatpants with stains on them, and a black Northface jacket. He was estimated to be about 5 feet 8 inches tall and about 140-150 pounds.

43. Victim manager and victim teller advised the UNSUB forced them behind the counter and made them give him the money from the cash register. Victim manager and victim teller stated the UNSUB told them not to use bait money or dye packs. UNSUB was given \$5,878.37 from the register. UNSUB directed the victim manager and victim teller to the “working vault” of the bank. From there he obtained over \$27,000.00. UNSUB requested the victim manager and victim teller open the vault that was on a time delay. When UNSUB was advised by the victim manager and victim teller of the fifteen minute time delay on the vault. UNSUB advised them that he would wait. After the vault opened, UNSUB took approximately \$128,000.00. UNSUB loaded the money into a box that he had emptied. UNSUB left the bank at approximately 8:17 a.m. and drove off in the white hatchback.

44. In total, UNSUB stole \$160,323.00 from the bank.

45. The vehicle UNSUB used during the bank robbery was consistent with a vehicle stolen at around 1:00 a.m. near the boat ramp, New Hampshire, and later recovered on the street in front of

New Hampshire. It is unknown when the vehicle was left in front of

but, according to Google Maps, the vehicle was found just over a two miles from the Bank of New England.

46. According to Google Maps, the boat ramp, New Hampshire (where the car was stolen), is located approximately at the following latitude and longitude:

47. According to Google Maps, New Hampshire (where the stolen car was found), is located approximately at the following latitude and longitude:

48. I have reviewed video or pictures from each of the above described robberies. Based on my review of the videos and photos, the UNSUB that committed each robbery appears to be the same individual. In particular the UNSUB has distinct eyebrows, nose, and general facial structure that appear the same in all the photos and videos.

49. Additionally, victims in all of the incidents described a very similar body type and build as well as similar behavior. Victims advised Manchester Police the UNSUB requested access to the safe in addition to the registers. For example, during the Rapid Refill robbery and Bank of New England robbery, the victims advised UNSUB that there was a time delay on the vault. In both situations UNSUB said he would wait for the time delay. Based on my training and experience, it is not common for a subject in a commercial robbery to show a willingness to wait for a vault with a time delay to open.

50. Ninety-six percent of American adults possess a cellular phone, and the substantial majority (81%) possess a “smartphone” (a phone capable of, among other things, connecting to the internet and downloading mobile applications).¹ Due to the ubiquity of the Google tools and services discussed above (*e.g.*, the free email and map applications, the

¹ See www.pewinternet.org/fact-sheet/mobile, last visited on January 3, 2020.

Android operating system, and the Google tools incorporated by advertisers and publishers into other web services and/or applications) and the fact that Google gathers data both actively and passively (even when the user is not engaged with the device), in my training and experience Google will have gathered data regarding substantial number of the cellular phone users in a particular location at a particular time.

51. Based on the foregoing, there is probable cause to search information in the possession of Google relating to what devices were in the Target Locations described in Attachment A during the time period described in Attachment A, as well as information that identifies the Google accounts with which those devices are associated, for evidence of the crimes at issue in this case. Among other things, this information can inculcate or exculpate a user of Google services by showing that he/she was (or was not) near a given location at a time relevant to the criminal investigation.

52. In order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates that Google will disclose the information to the government in stages rather than disclose all of the information for which the government has established probable cause to search at once. Specifically, as described in Attachment B.I:

- a. Google will be required to disclose to the government an anonymized list of devices that specifies the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available, of the devices that reported their location within the Target Locations described in Attachment A during the time period described in Attachment A.
- b. The government will then review this list in order to identify devices, if any, that it can determine are not likely to be relevant to the investigation (for example,

devices moving through the Target Locations in a manner inconsistent with the facts of the underlying case).

- c. Google will then be required to disclose to the government, at its request, the information identifying the Google account(s) to which remaining devices are associated.

CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

54. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING AND NONDISCLOSURE ORDER

55. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

56. I further request that, pursuant to the non-disclosure provisions of 18 U.S.C. §§ 2705(b), the Court order Google not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, the Order, or the execution of the warrant, for a period of one year from the date of this Order, or until notified by the government within thirty days of the conclusion of the investigation, whichever is earlier. Google may disclose this Order to an attorney for Google for the purposes of receiving legal advice.

57. Non-disclosure is appropriate in this case because the Court's order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the existence of the investigation. There is accordingly reason to believe that notification of the existence of the Order will seriously jeopardize the investigation, including by giving targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, or endanger the life or physical safety of an individual. See 18 U.S.C. § 2705(b).

Respectfully submitted,

/s/ Wesley R. Garland
Wesley R. Garland, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 7, 2020

/s/ Andrea K. Johnstone
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE